

Global Japanese Practice タイ アドバイザリー ニュースレター 2025 年 3 月 海外自動車部品工場におけるドイツ・情報セキュリティ認証 TISAX®取得事例の増加

お客様各位

平素はいつも大変お世話になっております。

自動車業界では、自動車メーカーの技術情報や顧客情報がサプライヤーと共有され、共同で部品開発やサービス提供が行われています。このサプライヤーに連携された情報を、セキュリティ上適切に取り扱うことを求めるため、ドイツ自動車工業会（VDA）は、TISAX®というセキュリティ認証の仕組みを策定しました。それを受け、日本のサプライヤーも、ドイツの自動車メーカーやサプライヤーから TISAX®認証取得を求められています。TISAX®では認証取得範囲を定める必要があり、近年では海外拠点も適用範囲に含める動きも活発化しています。一方で、日系サプライヤーも EV の台頭や自動車サプライチェーンの再編などを皮切りに顧客ポートフォリオの多層化を検討する企業も多く、ドイツや欧州系メーカーとの取引を継続・拡大する上では TISAX®の重要性はさらに高まってきています。

I. 「TISAX®」とは

TISAX®とは Trusted Information Security Assessment Exchange の略で 2017 年にドイツ自動車工業会（VDA）が策定した自動車産業における情報セキュリティの評価と共有のための認証制度になります。

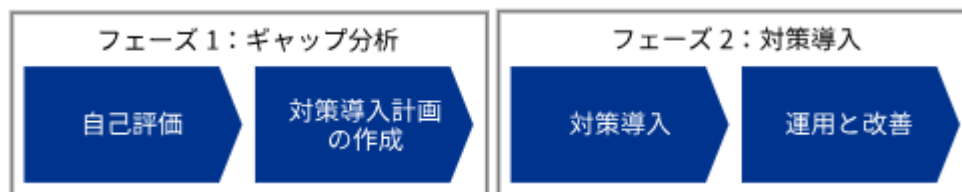
TISAX®認証は、ドイツ自動車工業会（VDA）に認定された審査機関のみが実施することができ、その結果は VDA に所属する自動車メーカーが共有することができます。また審査は英語またはドイツ語で実施されます。

TISAX®の要求事項は、情報セキュリティの国際規格である ISO/IEC 27000 シリーズの管理策がベースになっています。一方で、ISO/IEC 27001 の審査に比べて TISAX®審査では、要求事項を遵守する規定が整備されており、規定どおりに実際に運用されているかを、規定や運用の証跡を入手しての閲覧やインタビューで詳細に確認します。TISAX®では、各質問を 0 から 5 までの 6 段階の成熟度で評価し、合格ラインである 3 と評価されるためには、基本的に“Must”と“Should”の要求事項が規定として整備され、運用の証跡が存在しなければなりません。したがって、TISAX®対応のための ISMS は、ISO/IEC 27000 シリーズの管理策よりも、TISAX®のより具体的な要求事項に基づいて構築する必要があります。

II. TISAX®認証取得の進め方

TISAX®に対応するためには、自社の ISMS が TISAX®の要求事項と、どれくらいギャップがあるのかをまず把握する必要があります。フェーズ 1 でギャップを分析し、それを埋めるセキュリティ対策導入計画を作成することで、TISAX®対応の全体作業量が明確になります。フェーズ 2 では、セキュリティ対策導入計画に基づいて、TISAX®要求事項を遵守する規定や運用のための文書を整備し、規定通りに実際に運用・改善していきます。

自社の ISMS の成熟度や TISAX®認証取得の対象拠点の数にもよりますが、フェーズ 1 は 2～3 ヶ月で行います。その後のフェーズ 2 は、自社のセキュリティ対応の Кейパビリティや、外部からどこまでの支援を受けるか等にもよりますが、TISAX®の“Must”と“Should”の要求事項の数や ISO/IEC 27001 の認証取得の事例を踏まえると、文書を整備し、運用を定着させるために少なくとも半年～1 年以上は必要であると考えます。なお、海外拠点、特にタイをはじめとした東南アジアの生産事業体では、自前の情報セキュリティ部門も十分な人員がおらず、文書整備なども不十分なケースも散見されており、国内拠点以上に時間をかけた対応が必要になる可能性があります。



III. TISAX®審査

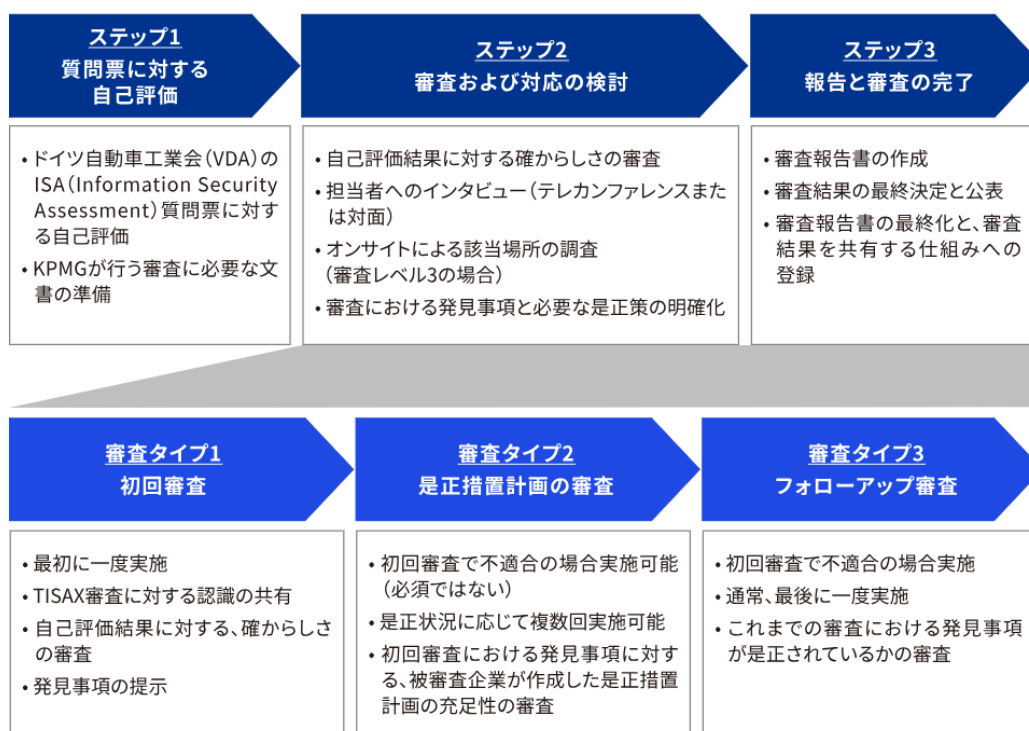
TISAX®は自己評価、審査機関による審査、審査結果の受領の流れ（下表1）となります。審査は英語またはドイツ語で実施され、12審査目的（下表2）について、被審査企業が審査レベル（下表3）を選択した上で審査を受けます。ただし、自己評価のみの審査レベル1は、通常はサプライヤーが自社の情報セキュリティレベルを確認する目的で利用することが多く、審査機関は自己評価結果を審査しないため、自動車メーカーからは審査レベル2または3の審査を求められることが一般的です。

審査レベル2や3の審査では、初回審査で適合（合格）、不適合（不合格）が示され、不適合の場合は発見事項が提示され、発見事項に対する是正措置計画書の提出および是正措置を実施していく必要があります。また是正結果については再度フォローアップ審査を受ける必要があります。

また審査報告書では以下の5つの要素について審査結果が報告されます。

- A. 審査関連情報：会社名、審査スコープ、審査対象、審査レベルなど
- B. 総合審査結果：審査結果（Conform、Minor Non-Conform、Major Non-Conform）、発見事項の数など
- C. 審査結果概要：情報セキュリティ管理の要求事項ごと（たとえば、アクセス制御）の評価結果など
- D. 審査結果詳細：すべての発見事項についての詳細な説明、対応するリスク評価結果、対応策など
- E. 情報セキュリティの成熟度：情報セキュリティ管理の要求事項ごとの成熟度

[表1：TISAX®審査の流れ]



[表 2：TISAX®審査目的と審査レベル]

#	審査目的	説明	審査レベル
1	Info high	保護ニーズの高い情報の取扱い（新規での選択は不可）	レベル2
2	Info very high	保護ニーズの非常に高い情報の取扱い（新規での選択は不可）	レベル3
3	Confidential	機密性の観点から、保護ニーズの高い情報の取扱い	レベル2
4	Strictly confidential	機密性の観点から、保護ニーズの非常に高い情報の取扱い	レベル3
5	High availability	可用性の観点から、保護ニーズの高い情報の取扱い	レベル2
6	Very high availability	可用性の観点から、保護ニーズの非常に高い情報の取扱い	レベル3
7	Proto parts	プロトタイプ部品・コンポーネントの保護	レベル3
8	Proto vehicles	プロトタイプ車両の保護	レベル3
9	Test vehicles	テスト車両の取扱い	レベル3
10	Proto events	イベントおよび動画・写真撮影時のプロトタイプの保護	レベル3
11	Data	GDPR第28条「処理者」に基づくデータ保護	レベル2
12	Special data	GDPR第9条に規定された 特別区分の個人データに関する、同第28条「処理者」に従ったデータの保護	レベル3

[表 3：審査レベルに対する審査方法]

審査レベル	自己評価	証拠の確認	インタビュー	オンサイトの審査
1 ³	必要	不要	不要	不要
2	必要	確からしさの検証	テレカンファレンス	状況に応じて実施
3	必要	詳細な検証	対面	必要

IV. KPMG の TISAX®関連サービス

KPMG では、ドイツ自動車工業会（VDA）認定の審査機関である KPMG ドイツを中心に、TISAX® 認証取得に関するアドバイザーサービスや審査サービスを提供しています。

TISAX®アドバイザーサービスでは、TISAX®の審査内容に精通した専門家による事前準備（適合状況の事前チェック、問題点の改善など）を通じて初回審査での適合（合格）判定の取得を支援します。また、審査は英語またはドイツ語での対応が求められますが、タイ国内においては KPMG タイのタイ人プロフェッショナルによるタイ語、英語でのサポートが可能です。

TISAX®審査サービスでは、認定審査機関である KPMG ドイツが審査をさせていただくことが可能です。KPMG ドイツは多くの日本企業の審査を実施した経験があり、日本企業の実態に即した適正かつ公正な審査が可能です。ただし、TISAX®アドバイザーサービスのご利用状況によっては、自己監査になってしまうため、KPMG ドイツが審査をできず、他の審査機関をご紹介させていただくケースもありますので詳細は担当者にご相談ください。

[KPMG ドイツの TISAX®審査サービス利用条件]

KPMG の TISAX®アドバイザーサービス		KPMG ドイツの TISAX®審査サービス
適合状況の事前チェック	問題点の改善支援	
利用なし	利用なし	可能
利用	利用なし	可能
利用	利用	不可
利用なし	利用	不可

KPMG 担当者

横山 大介
ディレクター
E: dyokoyama@kpmg.co.th



Woramon Sayalak
ディレクター
E: woramons@kpmg.co.th



[KPMG 日系企業支援サービスウェブサイト](#)
[過去のニューズレター一覧](#)

KPMG 日系企業サービス代表お問い合わせ先
gjp-marketing@kpmg.co.th

kpmg.com/th



[Privacy](#) | [Legal](#)

You have received this email from KPMG Phoomchai Holdings Co., Ltd. If you wish to unsubscribe from our mailing list, please [click here to unsubscribe](#).

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG Phoomchai Holdings Co., Ltd., a Thai limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization